Section C - Description/Specifications/Statement of Work

Statement of Work (SOW) for

Mission Critical Interior Communications (IC) Data Networks Support

1.0 INTRODUCTION

1.0.1 The Naval Surface Warfare Center Philadelphia Division (NSWCPD) is a Department of Defense entity responsible for research and development, test and evaluation, engineering and fleet support organization for the Navy's ships, submarines, military watercraft and unmanned vehicles. This requirement is for NSWCPD Code 52, which is responsible for the is-service engineering and lifecycle support for Mission Critical IC Data Networks.

1.0.2 This contract is for non-personal services. It does not create employment rights with the U.S. Government whether actual, inherent, or implied

1.0.3 Government/Contractor Relationship

1.0.3.1 The services to be delivered under this Task Order are non-personal services and the parties recognize and agree that no employer-employee relationship exists or will exist under the Task Order between the Government and the Contractor's personnel. Therefore, it is in the best interest of the Government to provide both parties a full understanding of their respective obligations.

1.0.3.2 The Contractor employees shall identify themselves as Contractor personnel by introducing themselves or being introduced as Contractor personnel and displaying distinguishable badges or other visible identification for meetings with Government personnel. In addition, Contractor personnel shall appropriately identify themselves as Contractor employees in telephone conversations and in formal and informal written correspondence.

1.0.3.3 Contractor personnel under this Task Order shall not engage in any of the inherently Governmental functions listed at FAR Subpart 7.5 or DFARS Subpart 207.5.

1.0.4 Employee Relationship:

1.0.4.1 The services to be performed under this Task Order do not require the Contractor or its personnel to exercise personal judgment and discretion on behalf of the Government. Rather the Contractor's personnel will act and exercise personal judgment and discretion on behalf of the Contractor.

1.0.4.2 Rules, regulations, directives, and requirements that are issued by the U. S. Navy and NSWCPD under its responsibility for good order, administration, and security are applicable to all personnel who enter a Government installation or who travel on Government transportation. This is not to be construed or interpreted to establish any degree of Government control that is inconsistent with a non-personal services contract.

1.0.4.3 Inapplicability of Employee Benefits: This Task Order does not create an employer-employee relationship. Accordingly, entitlements and

benefits applicable to such relationships do not apply.

1.0.4.4 It is the Contractor's, as well as the Government's, responsibility to

monitor Task Order activities and notify the Contracting Officer if the Contractor believes that the intent of this Section has been or may be violated.

1.0.4.4.1 The Contractor shall notify the Contracting Officer in writing via letter or email within three (3) calendar days from the date of any incident that the Contractor considers to constitute a violation of this Section. The notice should include the date, nature, and circumstances of the conduct; the name, function, and activity of each Government employee or Contractor official or employee involved or knowledgeable about such conduct; identify any documents or substance of any

oral communication involved in the conduct; and the Contractor's estimated date when, absent a response, cost, schedule or performance will be impacted.

1.0.4.4.2 The Contracting Officer will, within five (5) calendar days after receipt of notice, respond to the notice in writing. In responding, the Contracting Officer will either:

(i) Confirm the conduct is in violation and when necessary direct the mode of further performance,

(ii) Countermand any communication regarded as a violation,

(iii) Deny that the conduct constitutes a violation and when necessary direct the mode of further performance, or

(iv) In the event the notice is inadequate to make a decision, advise the Contractor what additional information is required, and establish the date by which it should be furnished by the Contractor.

1.1 BACKGROUND

The Cybersecure Machinery Control Systems & Networks Department (Code 50) at NSWCPD provides the facilities and expertise for developing the concepts, technologies, equipment, systems, and procedures necessary to enable current Navy ships to operate reliably, affordably and to effectively meet performance and mission requirements in a cybersecure manner. This knowledge of machinery systems engineering commences at the earliest stages of shipboard equipment and component product development, continues through new ship construction, and is maintained through In-Service Engineering (ISE) support to ships and ship systems currently in the Fleet. NSWCPD is an active participant in the community of world-class scientists and engineers that are developing the network-related technology and hardware needed to integrate shipboard systems in an increasingly net-centric Navy shipboard environment.

NSWCPD Codes 525 and 526 are the HM&E/Navigation Networks Branches within NSWCPD Division 52. These two branches provide lifecycle support for IC Data Networks installed on ships across the surface fleet and encompasses various Hull, Mechanical and Electrical (HM&E) Networks, Navigation Data Distribution Networks, Total Ship Computing Environment (TSCE) Networks and other network-based infrastructures used to facilitate communications amongst shipboard systems. These shipboard systems, often referred to as Network User Systems include but are not limited to Machinery Control, Ship Control, Damage Control, Electric Plant Control, Fuel Control, Condition Based Maintenance and Navigation Data Sources and Consumers.

NSWCPD Code 525 provides network design, integration and lifecycle ISE support for the USQ-82 Family of IC Data Networks installed primarily on DDG 51 Class Destroyers. NSWCPD Code 526 provides network design, integration and lifecycle ISE support across the surface fleet, with a focus on all other ship classes besides the DDG 51 Class. This contract will be used to provide support primarily for the networks and associated user systems under the cognizance of Code 526.

1.2 SCOPE OF WORK

The Contractor shall provide engineering and technical services required for the design, development, integration, configuration, testing, troubleshooting, repair, maintenance and fleet sustainment of IC Data Networks and associated user systems. The Contractor shall provide network hardware, software, and cybersecurity support services for IC Data networks designed, owned and/or ISE-supported by NSWCPD Codes 525/526 and installed at land-based engineering sites, labs, training facilities, and on operational hulls homeported and deployed around the world.

2.0 APPLICABLE DOCUMENTS

2.1 NSWCPD Systems Engineering Process (SEP) NSWC PHILADELPHIA DIV SOP 5400.00E.1 SEP Manual dated 1 September 2018

2.2 DON-IT Acceptable Use Policy Memorandum, dated 12 FEB 2016

2.3 NSWCPD Code 1043, “Media Scanning Between Boundaries Security Implementation Guide” Rev 4 (attached)

2.4 DoD 8140.01 Cyberspace Workforce Management requirement, dated 11 August 2015

2.5 NSWCPD Systems Engineering Process (SEP) Risk Assessment Plan, Rev: Basic, dated 7 July 2017

The Contractor shall reference and utilize the latest version available when performing tasks within this PWS.

3.0. REQUIREMENTS (CDRL A001)

3.1 Systems Engineering Support Services – NSWCPD performs analysis of functional, operational and environmental requirements for mission critical network conjunction with user system interface requirements and lifecycle lessons learned, to develop new network designs and/or upgrades to existing networks/systems eventual land-based engineering site and shipboard implementation. All related development, testing, shipboard installation and system lifecycle management executed in accordance with the NSWCPD Systems Engineering Process (SEP). To assist NSWCPD, the Contractor shall provide support in the following areas:

3.1.1 Network Architecture & Design Services –the Contractor shall assist in the development and/or modification of ship design specifications and in the review system specifications. The Contractor shall participate in associated System Design Reviews.

3.1.2 Software Engineering Services –the Contractor shall provide software design, development, testing and integration for the implementation of network fu requirements such as overall network management and equipment configuration management. The Contractor shall design software emulators used to re-crea shipboard systems.

3.1.3 Hardware Engineering Services –the Contractor shall provide engineering support for network products produced for labs, proof-of-concept demonstrat fielded shipboard systems. Work in this area includes initial concept exploration and requirements definition, through engineering development, qualificatio lab and/or shipboard integration, and troubleshooting.

3.2 Operational Support/Field Support Services –The availability, effectiveness, reliability, survivability and safety of shipboard and land-based mission critical networ and communication systems is necessary for the operational effectiveness of the Navy. NSWCPD is responsible to help ensure all systems under their cognizance a tested, installed, maintained and upgraded to sustain fleet mission readiness and capability. To support this mission, the Contractor shall provide support in t following areas:

3.2.1 Land-Based Engineering Site/Lab Support

3.2.1.1 The Contractor shall assist with the installation and initial checkout of new labs, including the successful integration of network user systems.

3.2.1.2 The Contractor shall assist with the development of network and network user system land-based test plans and procedures.

3.2.1.3 The Contractor shall assist with the execution of system audits, tests, and the verification & validation testing of network system-level and netv changes/upgrades prior to fleet delivery via approved Ship Change Documents (SCDs) or other installation vehicles.

3.2.1.4 The Contractor shall help troubleshoot failed land-based network equipment, interface cabling, and associated user systems.

3.2.1.5 The Contractor shall assist with the maintenance and upgrade of labs and network training sites.

3.2.2 Shipboard/Fleet Support

3.2.2.1 The Contractor shall troubleshoot and make minor repairs as permitted to failed shipboard network systems and associated user systems. The Cont in conjunction with Regional Maintenance Center (RMC) to every extent possible when working independent from an NSWCPD ISEA represen assistance may be provided via distance support, on a ship pier side or on a ship underway.

3.2.2.2 The Contractor shall install network configuration updates in support of network-level upgrades and/or user system installations, modifications, and ensure successful network performance and/or user system integration.

3.2.2.3 The Contractor shall support the installation and verification of network-related SCDs in accordance with Regional Maintenance and Modernizat Office (RMMCO) processes and procedures.

3.2.2.4 The Contractor shall support the installation and checkout of shipboard networks and user systems; tasking can include the removal and dis equipment, and the verification testing of upgraded equipment packages in compliance with the latest approved SCDs and system baseline.

3.2.2.5 The Contractor shall support the testing of in-process engineering change proposals (ECPs) or Temporary Alterations (TEMPALTs) in a shipb environment to help validate changes for permanent installation.

3.2.2.6 The Contractor shall provide informal shipboard system familiarization and training to ship's force personnel.

3.2.3 On-Site Installation Lead

3.2.3.1 The Contractor shall serve as the primary on-site installation lead for shipboard IC Data Network alterations & installations.

3.2.3.2 The Contractor shall act as the Network ISEA representative and provide oversight of alteration installation teams.

3.2.3.3 The Contractor shall assist the Government On-Site Installation Coordinator (OSIC) by verifying shipboard work is completed in accordance specifications, standards, controls, procedures, and policies and is in accordance with shipboard

installation drawings as well as ISEA recommendations, guidance, and

direction.

3.2.3.4 The Contractor shall develop & review Liaison Action Records (LARs) and work with the Planning Yard On-Site Representative for processing and

3.2.3.5 The Contractor shall participate in daily and weekly production meetings with the Government OSIC as the ISEA Representative and develop weel installation status briefs to be provided to ISEA, PMR, MSR, Shipyard reps, and others.

3.2.3.6 The Contractor shall review ship installation drawing packages for discrepancies, errors, omissions, and completeness and verify SIDs are develo ISEA provided technical data package.

3.2.3.7 The Contractor shall assist in development of installation technical data package generation and updates, including, but not limited to, identifying material specifications, part numbers, and methods.

3.2.3.8 The Contractor shall complete initial review of AIT Quality Assurance Workbooks.

3.3 Life Cycle System Support –As the lifecycle manager for IC Data Networks, NSWCPD is responsible for ensuring the long term sustainability of fielded lab a shipboard systems in order to reduce overall system total ownership costs for the Navy. To support this mission, the Contractor shall provide support in the followi areas:

3.3.1 The Contractor shall participate in System Program Reviews, Technical Reviews, Technical Exchange Meetings (TEMs), ISEA Team Meetings and other T and Programmatic forums to maintain awareness of program and system issues and initiatives.

3.3.2 The Contractor shall assist in the development of user manuals, technical descriptions, training material, and fact-sheets necessary for the sustained, su operation and maintenance of mission critical IC Data Networks.

3.3.3 The Contractor shall assist in the writing of SEP documents, requirements documents, test procedures and plans, test reports and other related documentation for lab, test site and shipboard applicability.

3.3.4 The Contractor shall help assess potential cost, schedule, and performance impact associated with the installation of proposed network hardware and changes.

3.4 Cybersecurity Support –As the ISEA and owner of IC Data Networks, NSWCPD is required to ensure its cognizant systems are assessed and authorized as part the development and acquisition process and throughout the system's operational lifecycle. To support this mission, the Contractor shall provide support in th following areas:

3.4.1 The Contractor shall assist in the development, verification, and continuous monitoring of system Authority To Operate (ATO) requests in accordance with Management Framework (RMF) requirements.

3.4.2 The Contractor shall assist in the development and/or integration of protect, detect, and response technologies to identify and mitigate cybersecurity vulnerab within shipboard networks and user systems.

3.4.3 The Contractor shall assist in the development, testing and fielding of software patches in support of emergent cybersecurity directives.

3.4.4 The Contractor shall provide Information Security Systems Manager (ISSM) support services, either by directly filling an ISSM billet or by reportin Government ISSM. The Contractor ISSM shall oversee and ensure that the appropriate operational security posture (e.g., network and system security, physic environmental protection, personnel security, incident handling, security training and awareness) is implemented and maintained for cognizant IC Data Netw The Contractor ISSM shall advise the ISEA, the Authorizing Official (AO) and information system owner on the security of mission critical IC Data Networks.

3.5 Administrative Assistant Support - Shall provide support to the Frigate, Guided Missile (FFG) X, LPD Flight I and II, CVN, DDG (X), DDG51 High Secur Firewall (HSF), CG, LSD, MCM, DDG1000, LHD, LCS 1 and 2 Class Ships. This effort shall consist of some technical but mostly programmatic support on the service and acquisition areas with the end goal to support each program network design & end-user system integration efforts, land based engineering site design testing, integrated logistics support, and cybersecurity support. Within those areas the contractor must support the programs listed above on performing reviev documentation, preparing reports, performing data collection and statistical analysis, perform financial support including man-hours/time related data, analysis a tracking.

3.5.1 Timekeeping – Weekly entering of all branch personnel time into ERP, routing leave/overtime requests.

3.5.2 Weekly Status Reports & Metrics - submitting status and metrics from all branch personnel to the Division on a weekly basis along with tracking.

3.5.3 Travel - reviewing travel orders for all branch personnel in the travel system DTS and tracking travel claims.

3.5.4 Records Management Assistance: Maintain Records Management compliance with the following but not limited to other documents that would be kept in accordance to records management guidance; SISO sheets; Correspondence, Memos, Delivery Letters, Telework Request/Agreements.

3.5.5 PS/LRVA/OH Error Reports – correcting timekeeping/NWA errors which show on these reports for all branch personnel.

3.5.6 Training – Tracking mandatory training for the branch, ESAMS, DAWIA & CSWF

3.5.7 Data Calls – Support answering data calls as they come in from both the Division, Department and/or command.

3.5.8 Public Release Approvals - work with all branch employees on routing for approvals.

3.5.9 Review and Update technical correspondence to ensure compliance with the Navy Correspondence Manual.

4.0 DATA REQUIREMENTS

4.1 Contract Status Report (CDRL A001)

4.1.1 This report shall reflect both prime and Subcontractor data if applicable at the same level of detail.

4.1.2 The CDRL shall be delivered electronically, unless otherwise stated, and while Contractor's format is acceptable the Government's approval must be received in writing from the COR within 5 business days before formal submission.

4.2 Travel Report (CDRL A002)

4.2.1 This report shall reflect both prime and subcontractor data if applicable at the same level of detail.

4.2.2 The CDRL shall be delivered electronically, unless otherwise stated, and while Contractor’s format is acceptable, Government’s approval is required from the COR.

4.3 Contractor’s Personnel Roster (CDRL A003)

4.3.1 The CDRL shall be delivered electronically, unless otherwise stated, and while Contractor’s format is acceptable, Government’s approval is required from the COR. This report shall reflect both prime and subcontractor data if applicable at the same level of detail.

4.4 Technical Reports (CDRL A004)

4.4.1 This report shall reflect both prime and subcontractor data if applicable at the same level of detail.

4.4.2 The CDRL shall be delivered electronically, and while Contractor’s format is acceptable, Government’s approval is required from the COR.

4.5 Government Property Inventory Report (CDRL A005)

4.5.1 This report shall reflect both prime and subcontractor data if applicable at the same level of detail.

4.5.2 The CDRL shall be delivered electronically, unless otherwise stated, and while Contractor’s format is acceptable, Government’s approval is required from the COR.

4.6 Small Business Utilization Report (CDRL A006)

4.6.1 This report shall reflect both prime and subcontractor data if applicable at the same level of detail.

4.6.2 The CDRL shall be delivered electronically, unless otherwise stated, and while Contractor’s format is acceptable, Government’s approval is required from the COR.

4.7 Systems Security Plan (CDRL A007)

4.7.1 This report shall reflect both prime and subcontractor data if applicable at the same level of detail.

4.7.2 The CDRL shall be delivered electronically, unless otherwise stated, and while Contractor's format is acceptable, Government's approval is required from the COR.

5.0 SECURITY REQUIREMENTS

5.1 SECURITY TRAINING. The Contractor is responsible for completing all required Government mandated training to maintain security and network access to government sites and IT systems to include but not limited to: Antiterrorism Level 1 Awareness; Records Management in the DON: Everyone's Responsibility; Training and Readiness: The Active Shooter; NAVSEA Introduction to Controlled Unclassified Information; Operations Security (OPSEC); NAVSEA Counterintelligence Training; Privacy and Personally Identifiable Information (PII) Awareness Training; NAVSEA Physical Security training and Cybersecurity 101 Training. Certificates of successful completion shall be sent to the COR and as otherwise specified in the contract.

5.1.1 In accordance with the NISPOM DoD 5220.22M, Contractor personnel that require access to Department of Navy (DON) information systems and/or work on-site require an open investigation or favorable adjudicated Tier 3 by the Vetting Risk Operations Center (VROC). An interim clearance is granted by VROC and recorded in the Joint Personnel Adjudication System (JPAS). An open or closed investigation with a favorable adjudication is required prior to issuance of a badge providing access to NSWCPD buildings. Furthermore, if the Navy Central Adjudication Facility, have made an unfavorable determination access will be denied. For Common Access Card (CAC) you must have an open investigation and or favorable adjusted investigation. Interim security clearance are acceptable for a CAC. Access will be denied for anyone that has eligibility pending in JPAS. Vetting through the National Crime Information Center, Sex Offender Registry, and the Terrorist screening database shall be process for a contractor that does not have a favorable adjudicated investigation.

5.1.2 Within 30 days after contract award, the contractor shall submit a list of all contractor personnel, including subcontractor employees, who will have access to DON information systems and/or work on-site at one of the NSWCPD sites to the appointed Contracting Officer Representative (COR) via email. The contractor shall provide each employee's first name, last name, contract number, the NSWCPD technical code, work location, whether or not the employee has a CAC and or Standard Access Control Badge (SACB), the systems the employee can access (i.e., NMCI, RDT&E), and the name of the Contractor's local point of contact, phone number and email address. Throughout the period of performance of the contract, the Contractor shall immediately provide any updated information to the COR when any Contractor personnel changes occur including substitutions or departures.

5.2 ON SITE WORK. Contractor personnel that require a badge to work on-site at one of the NSWCPD sites must provide an I-9 form to verify proof of citizenship. The I-9 form should be signed by the company Facility Security Officer or the company Human Resource Department. In addition to the I-9 form, Contractors shall also bring their birth certificate, current United States Passport or naturalization certificate and state issued ID to the NSWCPD Security Officer at the time of badge request to verify citizenship. Any contractor that has unfavorable information that has not been favorably adjudicated, by Department of Defense Central Adjudication Facility (DOD CAF) will not be issued a badge. Finally, contractors shall supply a copy of their OPSEC Training Certificate or other proof that the training has been completed.

5.2.1 In accordance with NSWCPD security protocol, contractor employees who hold dual citizenship will not be granted security clearance to our facilities.

5.3 DD254 REQUIREMENT. This effort may require access to classified information up to the Secret level. No classified data will be generated or stored by the Contractor. The Contractor is required to have and maintain a Secret clearance. The requirements of the attached DD Form 254 apply.

5.3.1 The contractor is required to maintain a Facility Security Clearance (FCL) in accordance with the DD254 to perform certain work under the contract. Although it is not required at time of award, it shall be obtained within 30 Days after award. Otherwise the government will have no obligation to continue ordering work under the contract and may not exercise any of the available options.

5.3.2 The Contractor shall appoint a Facility Security Officer (FSO), who shall (1) be responsible for all security aspects of the work performed under this contract, (2) assure compliance with the National Industrial Security Program Operating Manual (NISPOM) (DOD 5220.22-M), and (3) assure compliance with any written instructions from the NSWCPD, Security Office.

5.3.3 The contractor shall forward signed copies of DD254s provided to subcontractors to the Naval Surface Warfare Center Philadelphia Division (NSWCPD), ATTN: Security.

5.3.4 The contractor shall direct the subcontractor to obtain approval, through the prime Contractor, for the public release of information received or generated by the sub through the prime Contractor.

5.3.5 The contractor shall submit the subcontractor request for public release through the technical point of contact identified on the DD 254.

5.4 OPERATIONS SECURITY (OPSEC)

5.4.1 The Contractor shall protect critical information associated with this contract to prevent unauthorized disclosure. The NSWC Philadelphia Division's (NSWCPD) Critical Information List (CIL)/ CIIL (Critical Indicators and information list) will be provided on site, if warranted. Performance under this contract requires the contractor to adhere to OPSEC requirements. The Contractor may not impose OPSEC requirements on its subcontractors unless NSWCPD approves the OPSEC requirements. During the period of this contract, the Contractor may be exposed to, use, or produce, NSWCPD Critical Information (CI) and/or observables and indicators which may lead to discovery of CI. NSWCPD's CI will not be distributed to unauthorized third parties, including foreign governments, or companies under Foreign Ownership, Control, or Influence (FOCI).

5.4.2 CUI correspondence transmitted internally on the contractor's unclassified networks or information systems, and externally, shall be protected per NIST SP-800-171, Protecting Controlled Unclassified Information (CUI) in Non-federal Systems and Organizations.

Assembled large components/systems being transported to and from testing areas, other production or government facilities (whether or not on public roadways) shall be in an enclosed van trailer or covered flatbed trailer. Component/System outside storage, staging, and test areas shall be shielded/obscured from public view wherever physically possible.

5.4.3 NSWCPD's CI shall not be publicized in corporate wide newsletters, trade magazines, displays, intranet pages or public facing websites. Media requests related to this project shall be directed to the PCO, and the COR who will forward the required to the NSWCPD Public Release Authority for review.

5.4.4 Any attempt by unauthorized third parties to solicit, obtain, photograph, or record, or; incidents of loss/compromise of government Classified or CI, Business Sensitive, Company Proprietary information related to this or other program must be immediately reported to the contractor's Facility Security Officer and Cognizant Security Office and/or the Naval Criminal Investigative Service, and the NSWC PD Security Division (Code 105). Questions concerning these requirements shall be directed to the PCO, and the COR who will forward the request to the NSWC PD Security Division (Code 105).

5.5 RECEIPT, STORAGE, AND GENERATION OF CONTROLLED UNCLASSIFIED INFORMATION (CUI) All Controlled Unclassified Information (CUI) associated with this contract must follow the minimum marking requirements of DoDI 5200.48, Section 3, paragraph 3.4.a, and include the acronym "CUI" in the banner and footer of the document. In accordance with DoDI 5200.48, CUI must be safeguarded to prevent Unauthorized Disclosure (UD). CUI export controlled technical information or other scientific, technical, and engineering information must be marked with an export control warning as directed in DoDI 5230.24, DoDD 5230.25, and Part 250 of Title 32, CFR. Nonfederal information systems storing and processing CUI shall be protected per NIST SP-800-171, or subsequent revisions. All transmissions to personal email accounts (AOL, Yahoo, Hotmail, Comcast, etc.) and posting on social media websites (Facebook, Instagram, Twitter, LinkedIn, etc.) are prohibited. Destroy CUI associated with this contract by any of the following approved methods: A cross-cut shredder; a certified commercial destruction vendor; a central destruction facility; incineration; chemical decomposition; pulverizing, disintegration; or methods approved for classified destruction.

5.6 PLANNING, PROGRAMMING, BUDGETING AND EXECUTION (PPBE) DATA.

When contractor employees, in the performance of their duties, are exposed to Planning, Programming, Budgeting and Execution (PPBE) data, a Non-Disclosure Agreement (NDA) with all affected contactor personnel must be executed in coordination with the COR and PCO to ensure safeguarding disclosure of this data.

5.7 U-NNPI SECURITY REQUIREMENTS

5.7.1 Security Classification Guidance is as follows of portions of the tasking on

this contract when invoked in the task order statement of work:

5.7.1.1 Contractor requires access to information and equipment classified

at the Confidential National Security Information (NSI) level in order to provide industrial support services within facilities that actively supports the Navy Nuclear Propulsion Program (NNPP).

5.7.1.2 All contractor personnel accessing classified information or classified material associated with the performance of work related to the resultant contract must

be United States citizens, and shall have and maintain at a minimum Confidential security clearance.

5.7.1.3 The Contractor is responsible for completing all required government mandated training to maintain security and network access to government sites and IT systems, as necessary to support.

5.8 U-NNPI

5.8.1 Purpose The Contractor hereby agrees that when provided documents (specifications, drawings, etc.) that are marked as containing NOFORN sensitive information that must be controlled pursuant to Federal law, the information contained therein and generated as part of the inquiry shall be used only for the purpose stated in the contract and shall in no case be transmitted outside the company (unless such transmittals comply with the detailed guidance of the contract) or to any foreign national within the company. While in use, the documents shall be protected from unauthorized observation and shall be kept secure so as to preclude access by anyone not having a legitimate need to view them. The documents shall not be copied unless done in conformance with the detailed guidance of the contract. All the documents shall be promptly returned in their entirety, unless authorized for proper disposal or retention, following completion of the contract.

-

5.9.2 Specific Requirements for Protecting U-NNPI

a) Only U.S. citizens who have a need to know required to execute the contract shall be allowed access to U-NNPI.

b) When not in direct control of an authorized individual, U-NNPI must be secured in a locked container (e.g., file cabinet, desk, safe). Access to the container must be such that only authorized persons can access it, and compromise of the container would be obvious at sight. Containers should have no labels that indicate the contents. If removed from the site, U-NNPI must remain in the personal possession of the individual. At no time should U-NNPI be left unsecured (e.g., in a home c automobile, or unattended in a motel room or sent with baggage).

c) U-NNPI documents will have the word NOFORN at the top and bottom of each page. The cover sheet will have the warning statement shown below. Documents originated in the course of work that reproduce, expand or modify marked information shall be marked and controlled in the same way as the original. Media such a video tapes, disks, etc., must be marked and controlled similar to the markings on the original information.

d) U-NNPI may not be processed on networked computers with outside access unless approved by CNO (N00N). If desired, the company may submit a proposal for processing NNPI on company computer systems. Personally owned computing systems, such as personal computers, laptops, personal digital assistants, and other portable electronic devices are not authorized for processing NNPI. Exceptions require the specific approval of the cognizant DAA and CNO (N00N).

e) U-NNPI may be faxed within the continental United States and Hawaii provided there is an authorized individual waiting to receive the document and properly control it. U-NNPI may not be faxed to facilities outside the continental United States, including military installations, unless encrypted by means approved by CNC (N00N).

f) U-NNPI may be sent within the continental United States and Hawaii via first class mail in a single opaque envelope that has no markings indicating the nature of the contents.

g) Documents containing U-NNPI shall be disposed of as classified material.

h) Report any attempts to elicit U-NNPI by unauthorized persons to the appropriate security personnel.

i) Report any compromises of U-NNPI to the appropriate security personnel. This includes intentional or unintentional public release via such methods as theft, improper disposal (e.g., material not shredded, disks lost), placement on Web site, transmission via email, or violation of the information system containing U-NNPI

j) The only approved storage for U-NNPI is CDMS NOFORN.

6.0 PLACE OF PERFORMANCE

6.1 The contractor's primary place of performance shall be at government facilities in Philadelphia, PA and the Norfolk, VA area. It is estimated that 75% of the work will occur on-site at the NSWCPD facility, 10% at a Government facility in the Norfolk area, 10% at a Government facility in San Diego and 5% of the work will occur off-site at the contractor facility.

6.1.1 Performance will occur at the following government sites: NSWCPD facility in Philadelphia, PA, a Government facility in the Norfolk, VA area and a Government facility in San Diego County, CA.

6.1.2 Government will provide office space and phones/fax machines/computers/printers and phone/network connections for up to ten (10) Contractor personnel under this Contract. Note NMCI laptops and RDT&E laptops are considered GFP.

6.1.3 The specific location(s) will be provided at time of award of the Contract. The Contractor shall provide a list of employees who require access to these areas,

including standard security clearance information for each person, to the Contracting Officer Representative (COR) no later than three business days after the date of award. The work space provided to the Contractor personnel shall be identified by the Awardee, with appropriate signage listing the company name and individual Contractor employee name.

6.1.4 Access to Government buildings at Naval Surface Warfare Center Philadelphia Division is from 0600 to 1800 Monday through Friday, except Federal holidays. Normal work hours are from 0600 to 1800, Monday through Friday. Contractor employees shall be under Government oversight at all times. Government oversight requires that a Government employee be present in the same building/facility whenever Contractor employee(s) are performing work under this Contract. Contractor personnel are not allowed to access any Government buildings at NSWCPD outside the hours of 0600 to 1800 without the express approval of the Procuring Contracting Officer (PCO).

6.1.5 Early Dismissal and Closure of Government Facilities

6.1.5.1 When a Government facility is closed and/or early dismissal of Federal employees is directed due to severe weather, security threat, or a facility related problem that prevents personnel from working, onsite Contractor personnel regularly assigned to work at that facility should follow the same reporting and/or departure directions given to Government personnel. The Contractor shall not direct charge to the contract for time off, but shall follow its own company policies regarding leave. Non-essential Contractor personnel, who are not required to remain at or report to the facility, shall follow their parent company policy regarding whether they should go/stay home or report to another company facility. Subsequent to an early dismissal and during periods of inclement weather, onsite Contractors should monitor radio and television announcements before departing for work to determine if the facility is closed or operating on a delayed arrival basis.

6.1.5.2 When Federal employees are excused from work due to a holiday or a special event (that is unrelated to severe weather, a security threat, or a facility related problem), on site Contractors will continue working established work hours or take leave in accordance with parent company policy. Those Contractors who take leave shall not direct charge the non-working hours to the Contract. Contractors are responsible for predetermining and disclosing their charging practices for early dismissal, delayed openings, and closings in accordance with the FAR, applicable cost accounting standards, and company policy. Contractors shall follow their disclosed charging practices during the Contract period of performance, and shall not follow any verbal directions to the contrary. The PCO will make the determination of cost allowability for time lost due to facility closure in accordance with FAR, applicable Cost Accounting Standards, and the Contractor's established accounting policy.

6.1.6 The contractor shall ensure that each contractor employee who will be resident at NSWCPD completes the Environmental Management System (EMS) Awareness training within 30 days of commencing performance at NSWCPD. This document is available at: https://navsea navy.deps mil/wc/pnbc-code10/Safety /default.aspx

6.1.7 In accordance with C-223-W002, ON-SITE SAFETY REQUIREMENTS (NAVSEA), the contractor shall certify by email to (b)(6) (b)(6) that on-site employees have read the “Philadelphia Division Environmental Policy and Commitment” and taken the EMS Awareness training within 30 days of commencing performance at NSWCPD. The e-mail shall include the employee name, work site, and contract number.

7.0 TRAVEL

7.1 The Contractor may be required to travel from the primary performance location when supporting this requirement. The estimated average number of trips per year is 38; note that this will vary based on ship schedules, changes to ship schedules and unforeseen emergent technical support requests. The length of the trips will also vary based on the type of support that is required; for example, support for an emergent tech assist or straightforward SCD installation could take anywhere from 5-10 days while long term support for a modernization availability could last for weeks.

The contractor shall be required to travel CONUS and OCONUS (Hawaii and primarily Japan, the UAE and European countries) to accomplish the tasks contained in this contract. Travel in support of this requirement is anticipated to include, but may not be limited to, the following alternate performance locations (note that this table matches the base year requirement, but can vary thereafter):

CONUS/OCONUS	ORIGIN:	DESTINATION:	Number of Days Per Trip	Number of Trips	Number of People
CONUS	Philadelphia	Norfolk, VA	14	4	1
CONUS	Philadelphia	San Diego, CA	15	4	1

CONUS	Philadelphia	Mayport, FL	14	2	1
CONUS	Philadelphia	Pascagoula, MS	7	1	1
OCONUS	Philadelphia	Pearl Harbor, HI	14	1	1
OCONUS	Philadelphia	Sasebo, Japan	15	2	1
OCONUS	Philadelphia	Yokosuka. Japan	15	1	1
OCONUS	Philadelphia	Bahrain, UAE	15	1	1
CONUS	Norfolk	Mayport, FL	14	2	1
CONUS	Norfolk	San Diego, CA	15	4	1
CONUS	Norfolk	Philadelphia, PA	5	4	1
OCONUS	Norfolk	Pearl Harbor, HI	14	1	1
OCONUS	Norfolk	Sasebo, Japan	15	2	1
OCONUS	Norfolk	Bahrain, UAE	15	1	1
CONUS	San Diego	Philadelphia, PA	7	4	1
OCONUS	San Diego	Pearl Harbor, HI	14	2	1
OCONUS	San Diego	Sasebo, Japan	15	2	1
CONUS	Philadelphia	Washington, DC	14	2	1

7.2 The number of times the Contractor may be required to travel to each location cited above may vary as program requirements dictate, provided that the total estimated travel cost is not exceeded. The numbers of trips and types of personnel traveling shall be limited to the minimum required to accomplish work requirements. All travel shall be approved before travel occurs. Approval may be via email by the Contracting Officer (PCO) or the fully executed Technical Instruction (TI) signed by the Contracting Officer.

7.2.1 In accordance with the TI instructions, before initiating any travel the Contractor(s) shall submit a detailed and fully-burdened estimate that includes the number of employees traveling, their expected travel costs for airfare, lodging, per diem, rental car, taxi/mileage and any other costs or actions requiring approval. The travel estimate shall be submitted to the Contracting Officer's Representative (COR) and Contract Specialist. Actuals cost, resulting from the performance of travel requirements, shall be reported as part of the Contractor's monthly status report. The reportable cost shall also be traceable to the Contractor's invoice

7.3 All travel shall be conducted in accordance with FAR 31.205-46, Travel Costs, and B-231-H001 Travel Cost (NAVSEA) and shall be pre-approved by the COR. The Contractor shall submit travel reports in accordance with DI-MGMT-81943 (CDRL A002).

7.4 Travel Costs

-

7.4.1 The current “maximum per diem” rates are set forth in the (i) Federal Travel Regulations for travel in the Continental United States; (ii) Joint Travel Regulations for Overseas Non-Foreign areas (e.g., Alaska, Hawaii, Guam, Puerto Rico, etc.); and (ii) Department of State (DOS) prescribed rates for foreign overseas locations.

8.0 GOVERNMENT FURNISHED PROPERTY

~~**N/A**~~ The Government will be providing NMCI Laptops, RDT&E Laptops and External Hard drives as necessary under this Task Order.

9.0 GOVERNMENT FURNISHED INFORMATION

N/A

10.0 PURCHASES

10.1 Only items directly used and incidental to the services for this Task Order and for work within the scope of the Statement of Work, shall be purchased under the Other Direct Cost (ODC) line items. Purchases of an individual item that is valued above $10,000 shall be approved by the Contracting Officer prior to purchase by the Contractor. The purchase request and supporting documentation shall be submitted via email to the Contracting Officer and the Contracting Officer's Representative (COR) it shall be itemized and contain the cost or price analysis performed by the Contractor to determine the reasonableness of the pricing. Provide copies of price estimates from at least 2 vendors.

10.2 Information Technology (IT) equipment, or services must be approved by the proper approval authority. All IT requirements, regardless of dollar amount, submitted under this Task Order shall be submitted to the PCO for review and approval prior to purchase. The definition of information technology is identical to that of the Clinger-Cohen Act, that is, any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. Information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

11.0 COUNTERFEIT MATERIAL PREVENTION

11.1 Electronic End-Items

11.2 Non-Electronic Materiels

11.2.1 Department of the Navy contractors (and their subcontractors at all tiers)

who obtain critical or high risk materiel shall implement a risk mitigation process as follows:

11.2.1.1 If the materiel is currently in production or currently available, materiel shall be obtained only from authorized suppliers

11.2.1.2 If the materiel is not in production or currently available from authorized suppliers, materiel shall be obtained from suppliers that meet appropriate counterfeit avoidance criteria

11.2.1.3 Contractor shall notify the contracting officer when critical or high risk materiel cannot be obtained from an authorized supplier;

11.2.1.4 Contractor shall take mitigating actions to authenticate the materiel if purchased from an unauthorized supplier

11.2.1.5 Contractor shall report instances of counterfeit and suspect counterfeit materiel to the contracting officer and the GIDEP as soon as the contractor becomes aware of the issue.

12.0 PERSONNEL

12.1 Personnel Requirements. All persons proposed in key and non-key labor categories shall, at the time of proposal submission be U.S. citizens.

12.2 Clause 52.222-2 "Payment for Overtime Premiums" will provide for the total approved dollar amount of overtime premium or will state “zero” if not approved. If overtime premium has not been approved under this contract in accordance with Clause 52.222-2, overtime effort to be performed shall be requested from the Contracting Officer prior to performance of premium overtime. For overtime premium costs to be allowable costs; the Contracting Officer is required to approve the performance of overtime prior to the actual performance of overtime. The dollar amount in FAR 52.222-2 shall equal overtime premium negotiated between the Government and the prime contractor. This overtime premium amount shall equal the prime contractor's unburdened premium OT labor costs plus the subcontractors' fully-burdened premium OT labor costs.

12.3 The level of effort for the performance of the resultant Task Order is based on the following labor categories and hours per year:

Title	**eCRAFT Code**	**Key**	**GOVT-Site /KR-Site**	**Hours**	**Resumes Req**
Program/Project Manager II	MANP2	1	KR	640	1
Administrative Assistant	01020	0	GOVT	1920	0
Technical Writer III	30463	0	GOVT	2016	0
Information Systems Security Manager II	ISSM2	0	GOVT	2112	0
Computer Programmer IV	14074	0	GOVT	2112	0
Computer Engineer I	EC1	0	GOVT	4224	0
Computer Engineer II	EC2	0	GOVT	6336	0
Systems Engineer III	ESY3	0	GOVT	2112	0
Engineering Technician V	30085	0	GOVT	2208	0
Engineering Technician IV	30084	0	GOVT	2208	0

12.4 Key Personnel

Program/Project Manager II (1 resume):

Minimum Education: Bachelor's degree in Engineering or Business from an accredited college or university.

Target Experience: Five (5) years of experience as a Program Manager, to include contract and sub-contract management, budgeting, scheduling, planning, estimating, and progress. This individual should have experience in formulating, guiding, and directing the technical approach; and defining and negotiation with activity and agency personnel for necessary resources.

12.5 Non-Key Personnel

12.5.1 In the performance of this effort, the Contractor shall fully staff the non- key positions listed below with qualified individuals. The

Contractor shall provide individuals to fill the non-key positions identified below:

Administrative Assistant:

Minimum Education: High school/vocational school degree or GED certificate.

Minimum Experience: - Five (5) years of professional experience in secretarial/financial duties. This position will provide administrative support to executive staff with office management responsibilities to include budgeting, personnel records and payroll. The Administrative Assistant may be required to work independently on projects requiring research and preparation of briefing charts and other presentation materials.

Technical Writer III:

Minimum Education: Bachelor's level degree in any field from an accredited college or university.

Minimum Experience: Two (2) years experience in technical writing/editing. This individual should have experience writing and editing technical reports, brochures, and/or manuals for internal documentation, customer reference, or publication.

Information Systems Security Manager II:

Minimum Education: Bachelor’s Degree from accredited University or Certified Authorization Professional (CAP), CompTIA Advanced Security Practitioner (CASP) ce

CompTIA Security+ ce, Program Management Professional (PMP).

Minimum Experience: Validated 3-5 years specialized entry level experience providing the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security. This individual oversees and ensures that the appropriate operational security posture (e.g., network and system security, physical and environmental protection, personnel security, incident handling, security training and awareness) is implemented and maintained for an information system or program. Advises the Authorizing Official (AO), an information system owner, or the Chief Information Security Officer (CISO) on the security of an information system or program.

Computer Programmer IV:

Minimum Education: Bachelor's degree in a technical field from an accredited college or university.

Minimum Experience: Seven (7) years of computer programming experience. Applies expertise in programming procedures to complex programs; recommends the redesign of programs, investigates and analyzes feasibility and program requirements, develops programming specifications, and solves difficult programming problems. Uses knowledge of pertinent system software, computer equipment, work processes, regulations and management practices. Tests, documents, and writes operating instructions for all work. Works independently under overall objectives and direction, apprising the supervisor or team lead about progress and unusual complications.

Computer Engineer I:

Minimum Education: Bachelor's level degree in Computer, Electrical or Electronics Engineering or Mathematics from an accredited college or university.

Minimum Experience: No required professional experience.

Computer Engineer II:

Minimum Education: Bachelor's level degree in Computer, Electrical or Electronics Engineering or Mathematics from an accredited college or university.

Minimum Experience: Three (3) years of experience in the research, design, development, and/or testing of computer hardware or software programs, including product design, testing, implementation and maintenance.

Systems Engineer III:

Minimum Education: Bachelor's degree in Engineering from an accredited college or university.

Minimum Experience: Seven (7) years of experience in systems engineering, controls systems and/or networks. Has demonstrated the ability to independently apply complex engineering concepts to systems or network design, testing, troubleshooting and lifecycle maintenance requirements.

Engineering Technician V:

Minimum Education: High School/Vocational School Diploma or GED Certificate along with a Technical School Diploma.

Minimum Experience: Five (5) years work related experience in in the operation, maintenance, testing and troubleshooting of electrical/electronic systems and/or shipboard HM&E systems or networks. This individual should have experience checking and analyzing drawings or equipment to determine adequacy of drawings and design, determining test requirements, equipment modification, and test procedures and assisting with planning tests to evaluate equipment performance. Performs non-routine and complex assignments involving responsibility for planning and conducting a complete project of relatively limited scope or a portion of a larger and more diverse project.

Engineering Technician IV:

Minimum Education: High School/Vocational School Diploma or GED Certificate along with a Technical School Diploma or four (4) years Navy experience with C school training in an EM, ET, IC or IT rate specialty.

Minimum Experience: Four (4) years work related experience in in the operation, maintenance, testing and troubleshooting of electrical/electronic systems and/or shipboard electronic systems or networks. This individual should have experience checking and analyzing drawings or equipment to determine adequacy of drawings and design, determining test requirements, equipment modification, and test procedures and assisting with planning tests to evaluate equipment performance. Performs non-routine and complex assignments involving responsibility for planning and conducting a complete project of relatively limited scope or a portion of a larger and more diverse project.

12.6 DON Cyberspace IT (Information Technology) / Cybersecurity & Information Assurance Functions and Personnel Requirements

12.6.1 The table below outlines the requirements for the listed cyber positions: (

Position	CSWF Label**	CSWF Proficiency**	IAT or IAM Level (1,2,3)	IAWF Baseline Requirements	Operating System/Computing Environment(OS/CE) Qualification	IT Level (per SECNAV M-5510.30)

ISSM II	722 – Information Systems Security Manager	Intermediate/Journeyman	IAM-II	Bachelor Degree from accredited University or CAP, CASP ce, CompTIA Security+ ce, PMP	Directed by the Privileged Access Agreement	IT-II
Computer Programmer IV	621 – Software Developer	Intermediate/Journeyman	IAT-II	Bachelor Degree from accredited University or CSSLP	Directed by the Privileged Access Agreement	IT-II
Computer Engineer I	441 – Networks Operations Specialist	Advanced/ Master	IAT-II	Bachelor Degree from accredited University or CISSP, CASP ce	Directed by the Privileged Access Agreement	IT-II
Computer Engineer II						
Systems Engineer III						
Engineering Tech IV		Entry/ Apprentice		CompTIA A+ ce, CompTIA Network+ ce, SSCP		
Engineering Tech V						

13.0 NSWCPD ELECTRONIC COST REPORTING AND FINANCIAL TRACKING (ECRAFT) SYSTEM

13.1 In addition to the requirements of Clause C-237-W001 “Electronic Cost Reporting and Financial Tracking (eCRAFT) System Reporting (NAVSEA)”, the contractor is required to provide supporting accounting system reports, at the Contracting Officer’s request, based on the review of the invoice documentation submitted to eCRAFT. This documentation will include reports such as the Job Summary Report (or equivalent), Labor Distribution Report (or equivalent), and General Ledger Detail Report (or equivalent). Supporting labor data provided must include unburdened direct labor rates for each employee and labor category. Cost breakdowns for ODCs, Materials, travel and other non-labor costs must be at the transactional level in sufficient detail so the Government can review allocability to

the contract/task order. Indirect costs allocated to direct costs must be shown at the lowest level of detail sufficient to reconcile each indirect rate to the appropriate allocation base.

13.2 On invoices containing subcontractor costs, the prime contractor agrees, at the Contracting Officer's request, to attach as supporting documentation all invoices received from subcontractors, unless the subcontractor submits invoices directly to the CO and COR. This requirement applies to all subcontract types (Cost, FFP, etc.).

14.0 SPECIAL REQUIREMENTS

14.1 Quality Management System

14.1.1 The contractor shall maintain a Quality Management System (QMS) in accordance with ASQ/ANSI/ISO 9001:2015 standards per Naval Sea Systems Command (NAVSEA) QMS Acceptance Authority or appropriate directorate requirements. All QMS packages are required to adhere to applicable NAVSEA Technical Specification 9090-310 and NAVSEA Standard Item 009-04 requirements.

14.1.2 The contractor shall notify NSWCPD's Quality Department in writing when any changes are made to the QMS that may affect work defined in accordance with NAVSEA Technical Specification 9090-310.

14.1.3 The contractor shall ensure its QMS Level 3 specific work procedures relevant to the requirements of the Solicitation, including the SOW at the Task Order level (i.e. welding, etc.).

14.2 Risk Management

14.2.1 The contractor shall develop an internal risk management program and work jointly with the (Code 526) to develop an overall risk management program.

14.2.2 Assign responsibility for risk mitigation activities, and monitor progress through a formal tracking system.

14.2.3 Conduct risk identification and analysis during all phases of the program, including proposal development. Develop appropriate risk mitigation strategies and plans.

14.2.4 Use projected consequences of high probability risks to help establish the level of management reserve and schedule reserve.

14.2.5 Assess impact of identified performance, schedule and costs risks to estimate at completion, and include in the estimate as appropriate. Develop a range of estimates (best case, most likely, worst case).

14.2.6 The Contractor shall capture risks and associated mitigation plans in a risk database and provide status updates to the Government for all documented risks upon request.

C-202-H001 ADDITIONAL DEFINITIONS--BASIC (NAVSEA) (OCT 2018)

(a) Department - means the Department of the Navy.

(b) Commander, Naval Sea Systems Command - means the Commander of the Naval Sea Systems Command of the Department of the Navy or his duly appointed successor.

(c) References to The Federal Acquisition Regulation (FAR) - All references to the FAR in this contract shall be deemed to also reference the appropriate sections of the Defense FAR Supplement (DFARS), unless clearly indicated otherwise.

(d) National Stock Numbers - Whenever the term Federal Item Identification Number and its acronym FIIN or the term Federal Stock Number and its

acronym FSN appear in the contract, order or their cited specifications and standards, the terms and acronyms shall be interpreted as National Item Identification Number (NIIN) and National Stock Number (NSN) respectively which shall be defined as follows:

(1) National Item Identification Number (NIIN). The number assigned to each approved Item Identification under the Federal Cataloging Program. It consists of nine numeric characters, the first two of which are the National Codification Bureau (NCB) Code. The remaining positions consist of a seven digit non-significant number.

(2) National Stock Number (NSN). The National Stock Number (NSN) for an item of supply consists of the applicable four-position Federal Supply Class (FSC) plus the applicable nine-position NIIN assigned to the item of supply.

C-204-H001 USE OF NAVY SUPPORT CONTRACTORS FOR OFFICIAL CONTRACT FILES (NAVSEA) (OCT 2018)

(a) NAVSEA may use a file room management support contractor, hereinafter referred to as "the support contractor", to manage its file room, in which all official contract files, including the official file supporting this procurement, are retained. These official files may contain information that is considered a trade secret, proprietary, business sensitive or otherwise protected pursuant to law or regulation, hereinafter referred to as protected information. File room management services consist of any of the following: secretarial or clerical support; data entry; document reproduction, scanning, imaging, or destruction; operation, management, or maintenance of paper-based or electronic mail rooms, file rooms, or libraries; and supervision in connection with functions listed herein.

(b) The cognizant Contracting Officer will ensure that any NAVSEA contract under which these file room management services are acquired will contain a requirement that:

(1) The support contractor not disclose any information;

(2) Individual employees are to be instructed by the support contractor regarding the sensitivity of the official contract files;

(3) The support contractor performing these services be barred from providing any other supplies and/or services, or competing to do so, to NAVSEA for the period of performance of its contract and for an additional three years thereafter unless otherwise provided by law or regulation; and,

(4) In addition to any other rights the contractor may have, it is a third party beneficiary who has the right of direct action against the support of contractor, or any person to whom the support contractor has released or disclosed protected information, for the unauthorized duplication, release, or disclosure of such protected information.

(c) Execution of this contract by the contractor is considered consent to NAVSEA's permitting access to any information, irrespective of restrictive markings or the nature of the information submitted, by its file room management support contractor for the limited purpose of executing its file room support contract responsibilities.

(d) NAVSEA may, without further notice, enter into contracts with other contractors for these services. Contractors should enter into separate non-disclosure agreements with the file room contractor. Contact the Procuring Contracting Officer for contractor specifics. However, any such agreement will not be considered a prerequisite before information submitted is stored in the file room or otherwise encumber the government.

C-204-H002 IMPLEMENTATION OF ENHANCED SECURITY CONTROLS ON SELECT DEFENSE INDUSTRIAL BASE PARTNER NETWORKS (NAVSEA) (JAN 2020)

1. System Security Plan and Plans of Ace on and Milestones (SSP/POAM) Reviews

a) Within thirty (30) days of contract award, the Contractor shall make its System Security Plan(s) (SSP(s)) for its covered contractor information system(s) available for review by the Government at the contractor's facility. The SSP(s) shall implement the security requirements in Defense Federal Acquisition Regulae on Supplement (DFARS) clause 252.204-7012, which is included in this contract. The Contractor shall fully cooperate in the Government's review of the SSPs at the Contractor's facility.

b) If the Government determines that the SSP(s) does not adequately implement the requirements of DFARS clause 252.204-7012 then the Government shall notify the Contractor of each identified deficiency. The Contractor shall correct any identified deficiencies within thirty (30) days of notification by the Government. The contracting officer may provide for a correction period longer than thirty (30) days and, in such a case, may require the Contractor to submit a plan of action and milestones (POAM) for the correction of the identified deficiencies. The Contractor shall immediately notify the contracting officer of any failure or anticipated failure to meet a milestone in such a POAM.

c) Upon the conclusion of the correction period, the Government may conduct a follow-on review of the SSP(s) at the Contractor's facilities. The Government may continue to conduct follow-on reviews until the Government determines that the Contractor has corrected all identified deficiencies in the SSP(s).

d) The Government may, in its sole discretion, conduct subsequent reviews at the Contractor's site to verify the information in the SSP(s). The Government will conduct such reviews at least every three (3) years (measured from the date of contract award) and may conduct such reviews at any e me upon thirty (30) days' notice to the Contractor.

2. Compliance to NIST 800-171

a) The Contractor shall fully implement the CUI Security Requirements (Requirements) and associated Relevant Security Controls (Controls) in NIST Special Publication 800-171 (Rev. 1) (NIST SP 800-171), or establish a SSP(s) and POA&Ms that varies from NIST 800-171 only in accordance with DFARS clause 252.204-7012(b)(2), for all covered contractor information systems affecting this contract.

b) Notwithstanding the allowance for such variation, the contractor shall identify in any SSP and POA&M their plans to implement the following, at a minimum:

(1) Implement Control 3.5.3 (Multi-factor authentication). This means that multi-factor authentication is required for all users, privileged and unprivileged accounts that log into a network. In other words, any system that is not standalone should be required to utilize acceptable multi-factor authentication. For legacy systems and systems that cannot support this requirement, such as CNC equipment, etc., a combination of physical and logical protections acceptable to the Government may be substituted;

(2) Implement Control 3.1.5 (least privilege) and associated Controls, and identify practices that the contractor implements to restrict the unnecessary sharing with, or flow of, covered defense information to its subcontractors, suppliers, or vendors based on need-to-know principles;

(3) Implement Control 3.1.12 (monitoring and control remote access sessions) - Require monitoring and controlling of remote access sessions and include mechanisms to audit the sessions and methods.

(4) Audit user privileges on at least an annual basis;

(5) Implement:

i. Control 3.13.11 (FIPS 140-2 validated cryptology or implementation of NSA or NIST approved algorithms (i.e. FIPS 140-2 Annex A: AES or Triple DES) or compensating controls as documented in a SSP and POAM); and, ii. NIST Cryptographic Algorithm Validation Program (CAVP) (see https://csrc nist.gov/projects /cryptographic-algorithmvalidation-program);

(6) Implement Control 3.13.16 (Protect the confidentiality of CUI at rest) or provide a POAM for implementation which shall be evaluated by the Navy for risk acceptance.

(7) Implement Control 3.1.19 (encrypt CUI on mobile devices) or provide a plan of action for implementation which can be evaluated by the Government Program Manager for risk to the program.

3. Cyber Incident Response

a) The Contractor shall, within fifteen (15) days of discovering the cyber incident (inclusive of the 72-hour reporting period), deliver all data used in performance of the contract that the Contractor determines is impacted by the incident and begin assessment of potential warfighter/program impact.

b) Incident data shall be delivered in accordance with the Department of Defense Cyber Crimes Center (DC3) Instructions for Submitting Media available at http://www.acq.osd.mil/dpap/dars/pgi/docs/Instructions_for_Submiting_Media.docx In delivery of the incident data, the Contractor shall, to the extent practical, remove contractor-owned information from Government covered defense information.

c) If the Contractor subsequently identifies any such data not previously delivered to DC3, then the Contractor shall immediately notify the contracting officer in writing and shall deliver the incident data within ten (10) days of identification. In such a case, the Contractor may request a delivery date later than ten (10) days after identification. The contracting officer will approve or disapprove the request after coordination with DC3.

4. Naval Criminal Investigative Service (NCIS) Outreach

The Contractor shall engage with NCIS industry outreach efforts and consider recommendations for hardening of covered contractor information systems affecting DON programs and technologies.

5. NCIS/Industry Monitoring

a) In the event of a cyber incident or at any time the Government has indication of a vulnerability or potential vulnerability, the Contractor shall cooperate with the Naval Criminal Investigative Service (NCIS), which may include cooperation related to: threat indicators; pre-determined incident information derived from the Contractor's infrastructure systems; and the continuous provision of all Contractor, subcontractor or vendor logs that show network activity, including any additional logs the contractor, subcontractor or vendor agrees to initiate as a result of the cyber incident or notice of actual or potential vulnerability.

b) If the Government determines that the collection of all logs does not adequately protect its interests, the Contractor and NCIS will work together to implement additional measures, which may include allowing the installation of an appropriate network device that is owned and maintained by NCIS, on the Contractor's information systems or information technology assets. The specific details (e.g., type of device, type of data gathered, monitoring period) regarding the installation of an NCIS network device shall be the subject of a separate agreement negotiated between NCIS and the Contractor. In the alternative, the Contractor may install network sensor capabilities or a network monitoring service, either of which must be reviewed for acceptability by NCIS. Use of this alternative approach shall also be the subject of a separate agreement negotiated between NCIS and the Contractor.

c) In all cases, the collection or provision of data and any activities associated with this statement of work shall be in accordance with federal, state, and non-US law.

(End of Text)

C-211-H016 SPECIFICATIONS AND STANDARDS (NAVSEA) (OCT 2018)

(a) Definitions.

(i) A "zero-tier reference" is a specification, standard, or drawing that is cited in the contract (including its attachments).

(ii) A "first-tier reference" is either: (1) a specification, standard, or drawing cited in a zero-tier reference, or (2) a specification cited in a first-tier drawing.

(b) Requirements. All zero-tier and first-tier references, as defined above, are mandatory for use. All lower tier references shall be used for guidance only unless specifically identified below.

NONE

C-211-H017 UPDATING SPECIFICATIONS AND STANDARDS (NAVSEA) (DEC 2018)

The contractor may request that this contract be updated to include the current version of the applicable specification or standard if the update does not affect the form, fit or function of any deliverable item or increase the cost/price of the item to the Government. The contractor should submit update requests to the Procuring Contracting Officer with copies to the Administrative Contracting Officer and cognizant program office representative for approval. The contractor shall perform the contract in accordance with the existing specifications and standards until notified of approval/disapproval of its request to update by the Procuring Contracting Officer. Any approved alternate specifications or standards will be incorporated into the contract.

C-211-H018 APPROVAL BY THE GOVERNMENT (NAVSEA) (JAN 2019)

Approval by the Government as required under this contract and applicable specifications shall not relieve the Contractor of its obligation to comply with the specifications and with all other requirements of the contract, nor shall it impose upon the Government any liability it would not have had in the absence of such approval.

C-215-H002 CONTRACTOR PROPOSAL (NAVSEA) (OCT 2018)

(a) Performance of this contract by the Contractor shall be conducted and performed in accordance with detailed obligations to which the Contractor committed itself in Proposal dated 04 June 2021 in response to NAVSEA Solicitation No. N6449821R3015.

(b) The technical volume(s) of the Contractor's proposal is(are) hereby incorporated by reference and made subject to the "Order of Precedence" (FAR 52.215-8) clause of this contract. Under the "Order of Precedence" clause, the technical volume(s) of the Contractor's proposal referenced herein is (are) hereby designated as item (f) of the clause, following "the specifications" in the order of precedence.

(5) These conditions and controls are intended to serve as guidelines representing the minimum requirements of an acceptable ACP. They are not meant to restrict the Contractor in any way from imposing additional controls necessary to tailor these requirements to a specific facility.

(c) To request approval for non-U.S. citizens of hostile and/or communist-controlled countries (listed in Department of Defense Industrial Security Manual, DOD 5220.22-M or available from cognizant CAO), Contractor shall include in the ACP the following employee data: name, place of birth, citizenship (if different from

place of birth), date of entry to U.S., extenuating circumstances (if any) concerning immigration to U.S., number of years employed by Contractor, position, and stated intent concerning U.S. citizenship. COMNAVSEA or his designated representative will make individual determinations for desirability of access for the above group. Approval of ACP's for access of non-U.S. citizens of friendly countries will not be delayed for approval of non-U.S. citizens of hostile communist-controlled countries. Until approval is received, Contractor must deny access to vessels for employees who are non-U.S. citizens of hostile and/or communist-controlled countries.

(d) The Contractor shall fully comply with approved ACPs. Noncompliance by the Contractor or subcontractor serves to cancel any authorization previously granted, in which case the Contractor shall be precluded from the continued use of non-U.S. citizens on this contract or agreement until such time as the compliance with an approved ACP is demonstrated and upon a determination by the CAO that the Government's interests are protected. Further, the Government reserves the right to cancel previously granted authority when such cancellation is determined to be in the Government's best interest. Use of non-U.S. citizens, without an approved ACP or when a previous authorization has been canceled, will be considered a violation of security regulations. Upon confirmation by the CAO of such violation, this contract, agreement or any job order issued under this agreement may be terminated for default in accordance with the clause entitled "Default (Fixed-Price Supply And Service)" (FAR 52.249-8), "Default (Fixed-Price Research And Development)" (FAR 52.249-9) or "Termination (Cost Reimbursement)" (FAR 52.249-6), as applicable.

(e) Prime Contractors have full responsibility for the proper administration of the approved ACP for all work performed under this contract or agreement, regardless of the location of the vessel, and must ensure compliance by all subcontractors, technical representatives and other persons granted access to U.S. Navy vessels, adjacent areas, and work sites.

(f) In the event the Contractor does not intend to employ non-U.S. citizens in the performance of the work under this contract, but has non-U.S. citizen employees, such employees must be precluded from access to the vessel and its work site and those shops where work on the vessel's equipment is being performed. The ACP must spell out how non-U.S. citizens are excluded from access to contract work areas.

(g) The same restriction as in paragraph (f) above applies to other non-U.S. citizens who have access to the Contractor's facilities (e.g., for accomplishing facility improvements, from foreign crewed vessels within its facility, etc.) except that, with respect to access to the vessel and worksite, the restrictions shall not apply to uniformed U.S. Navy personnel who are non-U.S. citizens and who are either assigned to the ship or require access to the ship to perform their duties.

(End of Text)

C-223-W002 ON-SITE SAFETY REQUIREMENTS (NAVSEA) (OCT 2018)

(a) The contractor shall ensure that each contractor employee reads any necessary safety documents within 30 days of commencing performance at any Government facility. Required safety documents can be obtained from the respective safety office. Contractors shall notify the Safety office points of contact below to report completion of the required training via email. The email shall include the contractor employees name, work site, and contract number.

(b) It is expected that contractor employees will have received training from their employer on hazards associated with the areas in which they will be working and know what to do in order to protect themselves. Contractors are required to adhere to the requirements of 29 CFR 1910, 29 CFR 1926 and applicable state and local requirements while in Government spaces. The contractor shall ensure that all on-site contractor work at the Government facility is in accordance with any local safety instructions as provided via the COR. The contractor shall report all work-related injuries/illnesses that occurred while working at the Government site to the COR.

(c) Contractors whose employees perform work within Government spaces in excess of 1000 hours per calendar quarter during a calendar year shall submit the data elements on OSHA Form 300A, Summary of Work Related Injuries and Illnesses, for those employees to the safety office, via the COR by 15 January for the previous calendar year, even if no work related injuries or illnesses occurred. If a contractors injury/illness rates are above the Bureau of Labor Statistics industry standards, a safety assessment may be performed by the Safety Office to determine if any administrative or engineering controls can be utilized to prevent further injuries/illnesses, or if any additional Personal Protective Equipment or training will be required.

(d) Any contractor employee exhibiting unsafe behavior may be removed from the Government site. Such removal shall not relieve the contractor from meeting its contractual obligations and shall not be considered an excusable delay as defined in FAR 52.249-14.

(e) The Safety Office points of contacts are as follows:

(b)(6) and (b)(6)

C-227-H006 DATA REQUIREMENTS (NAVSEA) (OCT 2018)

The data to be furnished hereunder shall be prepared in accordance with the Contract Data Requirements List, DD Form 1423, Exhibit(s) A through H , attached hereto.

C-227-H008 GOVERNMENT-INDUSTRY DATA EXCHANGE PROGRAM (NAVSEA) (DEC 2018)

(a) The contractor shall actively participate in the Government Industry Data Exchange Program in accordance with the GIDEP Operations Manual, S0300-BT-PRO-010. The contractor shall submit information concerning critical or major nonconformances, as defined in FAR 46.407/DFARS 246.407, to the GIDEP information system.

(b) The contractor shall insert paragraph (a) of this clause in any subcontract when deemed necessary. When so inserted, the word "contractor" shall be changed to "subcontractor."

(c) The contractor shall, when it elects not to insert paragraph (a) in a subcontract, provide the subcontractor any GIDEP data which may be pertinent to items of its manufacture and verify that the subcontractor utilizes any such data.

(d) The contractor shall, whether it elects to insert paragraph (a) in a subcontract or not, verify that the subcontractor utilizes and provides feedback on any GIDEP data that may be pertinent to items of its manufacture."

(e) GIDEP materials, software and information are available without charge from:

GIDEP Operations Center
P.O. Box 8000
Corona, CA 92878-8000
Phone: (951) 898-3207
FAX: (951) 898-3250
Internet: http://www.gidep.org

(End of text)

C-227-H014 PROTECTION OF DEPARTMENT OF NAVY TRADEMARKS - BASIC (NAVSEA) (NOV 2020)

(a) The Contractor shall not assert any claim, in any jurisdiction, including but not limited to trademark infringement, based on rights the Contractor believes it has in the term(s) against the Government or others authorized by the Government to use the Designation(s) (including the word(s), name, symbol, or design). The Contractor may not use the Designation(s) (including the word(s), name, symbol, or design) alone or in combination with other words or numbers without prior written permission from the Government.

(b) The Government is providing the Designation(s) to the Contractor for use in connection with, and only in connection with, the activities relating to the manufacture, production, distribution, use, and packaging of the products and services identified under this contract. The Contractor shall not use the Designations for any other purpose without the prior written permission of the Contracting Officer.

(c) The Contractor shall notify the Contracting Officer of any intent it might have to assert rights in, or file an application to register, any one of the Designation(s) in any jurisdiction. Any such notification shall be in writing and shall identify the Designation(s) (including the word(s), name, symbol, or design), provide a statement as to its intended use(s) in commerce, and list the particular classes of goods or services in which registration will be sought.

(d) The Contractor shall ensure that any use of the Designation(s) by contractor will inure to the benefit of the Government.

(e) The Contractor acknowledges that these obligations with respect to the Designation(s) shall survive the expiration, completion, closeout, or termination of this contract.

(End of Text)

C-237-H001 SERVICE CONTRACT REPORTING (NAVSEA) (JAN 2021)

(a) Services Contract Reporting (SCR) requirements apply to this contract. The contractor shall report required SCR data fields using the SCR section of the System for Award Management (SAM) at following web address: https://sam.gov/SAM/.

(b) Reporting inputs will be for the labor executed during the period of performance during each Government fiscal year (FY), which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported no later than October 31 of each calendar year. Contractors may direct questions to the help desk, linked at https://sam.gov/SAM/.

(End of Text)

C-237-H002 SUBSTITUTION OF KEY PERSONNEL (NAVSEA) (OCT 2018)

(a) The Contractor agrees that a partial basis for award of this contract is the list of key personnel proposed. Accordingly, the Contractor agrees to assign to this contract those key persons whose resumes were submitted with the proposal necessary to fulfill the requirements of the contract. No substitution shall be made without prior notification to and concurrence of the Contracting Officer in accordance with this requirement. Substitution shall include, but not be limited to, subdividing hours of any key personnel and assigning or allocating those hours to another individual not approved as key personnel.

(b) All proposed substitutes shall have qualifications equal to or higher than the qualifications of the person to be replaced. The Contracting Officer shall be notified in writing of any proposed substitution at least forty-five (45) days, or ninety (90) days if a security clearance is to be obtained, in advance of the proposed substitution. Such notification shall include: (1) an explanation of the circumstances necessitating the substitution; (2) a complete resume of the proposed substitute; (3) an explanation as to why the proposed substitute is considered to have equal or better qualifications than the person being replaced; (4) payroll record of the proposed replacement; and (5) any other information requested by the Contracting Officer to enable him/her to judge whether or not the Contractor is maintaining the same high quality of personnel that provided the partial basis for award.

(c) Key personnel are identified in an attachment in Section J.

C-237-W001 ELECTRONIC COST REPORTING AND FINANCIAL TRACKING (eCRAFT) SYSTEM REPORTING (NAVSEA) (APR 2019)

(a) The Contractor agrees to upload the Contractor's Funds and Man-hour Expenditure Reports in the Electronic Cost Reporting and Financial Tracking (eCRAFT) System and submit the ContractorÆs Performance Report on the day and for the same timeframe the contractor submits an invoice into the Wide Area Workflow (WAWF) module on the Procurement Integrated Enterprise Environment (PIEE) system. Compliance with this requirement is a material requirement of this contract. Failure to comply with this requirement may result in contract termination.

(b) The Contract Status Report indicates the progress of work and the status of the program and of all assigned tasks. It informs the Government of existing or potential problem areas.

(c) The ContractorÆs Fund and Man-hour Expenditure Report reports contractor expenditures for labor, materials, travel, subcontractor usage, and other contract charges.

(1) Access: eCRAFT: Reports are uploaded through the eCRAFT System Periodic Report Utility (EPRU). The EPRU spreadsheet and user manual can be obtained at: http://www navsea.navy mil/Home/Warfare-Centers/NUWC-Newport/Partnerships/Commercial-Contracts/Information-eCraft-/ under eCRAFT information. The link for eCRAFT report submission is: https://www.pdrep.csd.disa mil/pdrep_files/other/ecraft htm. If you have problems uploading reports, please see the Frequently Asked Questions at the site address above.

(2) Submission and Acceptance/Rejection: Submission and Acceptance/Rejection: The contractor shall submit their reports on the same day and for the same timeframe the contractor submits an invoice in iRAPT. The amounts shall be the same. eCRAFT acceptance/rejection will be indicated by e-mail notification from eCRAFT.

C-242-H001 EXPEDITING CONTRACT CLOSEOUT (NAVSEA) (OCT 2018)

(a) As part of the negotiated fixed price or total estimated amount of this contract, both the Government and the Contractor have agreed to waive any entitlement that otherwise might accrue to either party in any residual dollar amount of $1,000 or less at the time of final contract closeout. The term "residual dollar amount" shall include all money that would otherwise be owed to either party at the end of the contract, except that, amounts connected in any way with taxation, allegations of fraud and/or antitrust violations shall be excluded. For purposes of determining residual dollar amounts, offsets of money owed by one party against money that would otherwise be paid by that party may be considered to the extent permitted by law.

(b) This agreement to waive entitlement to residual dollar amounts has been considered by both parties. It is agreed that the administrative costs for either party associated with collecting such small dollar amounts could exceed the amount to be recovered.

C-242-H002 POST AWARD MEETNG (NAVSEA) (OCT 2018)

(a) A post-award meeting with the successful offeror will be conducted within thirty (30) calendar days after award of the Task order. The meeting will be held at the address below:

Location/Address: via teleconference*

(b) The contractor will be given at least ten (10) working days notice prior to the date of the meeting by the Contracting Officer.

(c) The requirement for a post-award meeting shall in no event constitute grounds for excusable delay by the contractor in performance of any provisions in the Task Order.

(d) The post-award meeting will include, but is not limited to, the establishment of work level points of contact, determining the administration strategy, roles and responsibilities, and ensure prompt payment and close out. Specific topics shall be mutually agreed to prior to the meeting.

[*] Information will be provided by the Contract Specialist/Contracting Officer after Task Order award.

C-242-H003 TECHNICAL INSTRUCTIONS (NAVSEA) (OCT 2018)

(a) Performance of the work hereunder may be subject to written technical instructions signed by the Contracting Officer and the Contracting Officer's Representative specified in Section G of this contract. As used herein, technical instructions are defined to include the following:

(1) Directions to the Contractor which suggest pursuit of certain lines of inquiry, shift work emphasis, fill in details or otherwise serve to accomplish the contractual statement of work.

(2) Guidelines to the Contractor which assist in the interpretation of drawings, specifications or technical portions of work description.

(b) Technical instructions must be within the general scope of work stated in the contract. Technical instructions may not be used to: (1) assign additional work under the contract; (2) direct a change as defined in the "CHANGES" clause of this contract; (3) increase or decrease the contract price or estimated contract amount (including fee), as applicable, the level of effort, or the time required for contract performance; or (4) change any of the terms, conditions or specifications of the contract.

(c) If, in the opinion of the Contractor, any technical instruction calls for effort outside the scope of the contract or is inconsistent with this requirement, the Contractor shall notify the Contracting Officer in writing within ten (10) working days after the receipt of any such instruction. The Contractor shall not proceed with the work affected by the technical instruction unless and until the Contractor is notified by the Contracting Officer that the technical instruction is within the scope of this contract.

(d) Nothing in the foregoing paragraph shall be construed to excuse the Contractor from performing that portion of the contractual work statement which is not affected by the disputed technical instruction.

C-244-H002 SUBCONTRACTORS/CONSULTANTS (NAVSEA) (OCT 2018)

Notwithstanding FAR 52.244-2(d) and in addition to the information required by FAR 52.244-2(e) of the contract, the contractor shall include the following information in requests to add subcontractors or consultants during performance, regardless of subcontract type or pricing arrangement:

(1) Impact on subcontracting goals,

(2) Impact on providing support at the contracted value,

(3) IF SEAPORT TASK ORDER - The results of negotiations to incorporate fee rate caps no higher than the lower of (i) SeaPort-NXG fee rate caps for the prime contractor, or in the case where the proposed subcontractor is also a SeaPort-NXG prime, (ii) fee rate caps that are no higher than the subcontractor's prime SeaPort-NXG contract.

C-245-H005 INFORMATION AND DATA FURNISHED BY THE GOVERNMENT--ALTERNATE I (NAVSEA) (MAR 2019)

(a) Contract Specifications, Drawings and Data. The Government will furnish, if not included as an attachment to the contract, any unique contract specifications or other design or alteration data cited or referenced in Section C.

(b) Government Furnished Information (GFI). GFI is defined as that information essential for the installation, test, operation, and interface support of all Government Furnished Material identified in an attachment in Section J. The Government shall furnish only the GFI identified in an attachment in Section J. The GFI furnished to the contractor need not be in any particular format. Further, the Government reserves the right to revise the listing of GFI as follows:

(1) The Contracting Officer may at any time by written order:

(i) delete, supersede, or revise, in whole or in part, data identified in an attachment in Section J; or

(ii) add items of data or information to the attachment identified in Section J; or

(iii) establish or revise due dates for items of data or information in the attachment identified in Section J.

(2) If any action taken by the Contracting Officer pursuant to subparagraph (1) immediately above causes an increase or decrease in the costs of, or the time required for, performance of any part of the work under this contract, the contractor may be entitled to an equitable adjustment in the contract amount and delivery schedule in accordance with the procedures provided for in the "CHANGES" clause of this contract.

(c) Except for the Government information and data specified by paragraphs (a) and (b) above, the Government will not be obligated to furnish the Contractor any specification, standard, drawing, technical documentation, or other publication, notwithstanding anything to the contrary in the contract specifications, the GFI identified in an attachment in Section J, the clause of this contract entitled "Government Property" (FAR 52.245-1) or "Government Property Installation Operation Services" (FAR 52.245-2), as applicable, or any other term or condition of this contract. Such referenced documentation may be obtained:

(1) From the ASSIST database via the internet at http://assist.daps.dla mil/; or

(2) By submitting a request to the

Department of Defense Single Stock Point (DoDSSP) Building 4, Section D

700 Robbins Avenue

Philadelphia, Pennsylvania 19111-5094

Telephone (215) 697-6396

Facsimile (215) 697-9398

Commercial specifications and standards, which may be referenced in the contract specification or any sub-tier specification or standard, are not available from Government sources and should be obtained from the publishers.

C-247-H001 PERMITS AND RESPONSIBILITIES (NAVSEA) (DEC 2018)

The Contractor shall, without additional expense to the Government, be responsible for obtaining any necessary licenses and permits for complying with any applicable Federal, State, and Municipal laws, codes, and regulations for shipping and transportation including, but not limited to, any movement over public highways of overweight/over dimensional materials.

(End of Text)